

EL465777275

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

* * * * *

METHOD OF ADDRESSING MESSAGES AND
COMMUNICATIONS SYSTEM

* * * * *

INVENTOR

CLIFTON W. WOOD, JR.

ATTORNEY'S DOCKET NO. MI40-089

EM156304181

METHOD OF ADDRESSING MESSAGES AND COMMUNICATIONS SYSTEM

TECHNICAL FIELD

This invention relates to communications protocols and to digital data communications. Still more particularly, the invention relates to data communications protocols in mediums such as radio communication or the like. The invention also relates to radio frequency identification devices for inventory control, object monitoring, determining the existence, location or movement of objects, or for remote automated payment.

BACKGROUND OF THE INVENTION

Communications protocols are used in various applications. For example, communications protocols can be used in electronic identification systems. As large numbers of objects are moved in inventory, product manufacturing, and merchandising operations, there is a continuous challenge to accurately monitor the location and flow of objects. Additionally, there is a continuing goal to interrogate the location of objects in an inexpensive and streamlined manner. One way of tracking objects is with an electronic identification system.

One presently available electronic identification system utilizes a magnetic coupling system. In some cases, an identification device may be provided with a unique identification code in order

1 to distinguish between a number of different devices. Typically,
2 the devices are entirely passive (have no power supply), which
3 results in a small and portable package. However, such
4 identification systems are only capable of operation over a
5 relatively short range, limited by the size of a magnetic field used
6 to supply power to the devices and to communicate with the
7 devices.

8 Another wireless electronic identification system utilizes a
9 large active transponder device affixed to an object to be monitored
10 which receives a signal from an interrogator. The device receives
11 the signal, then generates and transmits a responsive signal. The
12 interrogation signal and the responsive signal are typically radio-
13 frequency (RF) signals produced by an RF transmitter circuit.
14 Because active devices have their own power sources, and do not
15 need to be in close proximity to an interrogator or reader to
16 receive power via magnetic coupling. Therefore, active transponder
17 devices tend to be more suitable for applications requiring tracking
18 of a tagged device that may not be in close proximity to an
19 interrogator. For example, active transponder devices tend to be
20 more suitable for inventory control or tracking.

21 Electronic identification systems can also be used for remote
22 payment. For example, when a radio frequency identification
23 device passes an interrogator at a toll booth, the toll booth can
24 determine the identity of the radio frequency identification device,

1 and thus of the owner of the device, and debit an account held by
2 the owner for payment of toll or can receive a credit card number
3 against which the toll can be charged. Similarly, remote payment
4 is possible for a variety of other goods or services.

5 A communication system, such as a wireless identification
6 system, typically includes two transponders: a commander station or
7 interrogator, and a responder station or transponder device which
8 replies to the interrogator.

9 If the interrogator has prior knowledge of the identification
10 number of a device which the interrogator is looking for, it can
11 specify that a response is requested only from the device with that
12 identification number. Sometimes, such information is not
13 available. For example, there are occasions where the interrogator
14 is attempting to determine which of multiple devices are within
15 communication range.

16 When the interrogator sends a message to a transponder
17 device requesting a reply, there is a possibility that multiple
18 transponder devices will attempt to respond simultaneously, causing
19 a collision, and thus an erroneous message to be received by the
20 interrogator. For example, if the interrogator sends out a command
21 requesting that all devices within a communications range identify
22 themselves, and gets a large number of simultaneous replies, the
23 interrogator may not be able to interpret any of these replies. Thus,
24

1 arbitration schemes are employed to permit communications free of
2 collisions.

3 In one arbitration scheme or system, described in commonly
4 assigned U.S. Patent Nos. 5,627,544; 5,583,850; 5,500,650; and
5 5,365,551, all to Snodgrass et al. and all incorporated herein by
6 reference, the interrogator sends a command causing each device of
7 a potentially large number of responding devices to select a random
8 number from a known range and use it as that device's arbitration
9 number. By transmitting requests for identification to various
10 subsets of the full range of arbitration numbers, and checking for
11 an error-free response, the interrogator determines the arbitration
12 number of every responder station capable of communicating at the
13 same time. Therefore, the interrogator is able to conduct
14 subsequent uninterrupted communication with devices, one at a time,
15 by addressing only one device.

16 Another arbitration scheme is referred to as the Aloha or
17 slotted Aloha scheme. This scheme is discussed in various
18 references relating to communications, such as Digital
19 Communications: Fundamentals and Applications, Bernard Sklar,
20 published January 1988 by Prentice Hall. In this type of scheme,
21 a device will respond to an interrogator using one of many time
22 domain slots selected randomly by the device. A problem with the
23 Aloha scheme is that if there are many devices, or potentially
24 many devices in the field (i.e. in communications range, capable

1 of responding) then there must be many available slots or many
2 collisions will occur. Having many available slots slows down
3 replies. If the magnitude of the number of devices in a field is
4 unknown, then many slots are needed. This results in the system
5 slowing down significantly because the reply time equals the
6 number of slots multiplied by the time period required for one
7 reply.

8 An electronic identification system which can be used as a
9 radio frequency identification device, arbitration schemes, and
10 various applications for such devices are described in detail in
11 commonly assigned U.S. Patent Application Serial Number
12 08/705,043, filed August 29, 1996, and incorporated herein by
13 reference.
14

15 SUMMARY OF THE INVENTION

16 The invention provides a wireless identification device
17 configured to provide a signal to identify the device in response
18 to an interrogation signal.

19 One aspect of the invention provides a method of establishing
20 wireless communications between an interrogator and individual ones
21 of multiple wireless identification devices. Tree search and Aloha
22 methods are combined to establish communications between the
23 interrogator and individual ones of the multiple wireless
24 identification devices without collision.

1 One aspect of the invention provides a method of addressing
2 messages from an interrogator to a selected one or more of a
3 number of communications devices. A first predetermined number
4 of bits are established to be used as unique identification numbers.
5 Unique identification numbers respectively having the first
6 predetermined number of bits are established for respective devices.
7 A second predetermined number of bits are established to be used
8 for random values. The devices are caused to select random
9 values. Respective devices choose random values independently of
10 random values selected by the other devices. The interrogator
11 transmits a command requesting devices having random values
12 within a specified group of random values to respond, the specified
13 group being less than or equal to the entire set of random values.
14 Devices receiving the command respectively determine if their
15 chosen random values fall within the specified group and, if so,
16 send a reply to the interrogator within a randomly selected time
17 slot of a number of slots. If not, they do not send a reply. The
18 interrogator determines if a collision occurred between devices that
19 sent a reply and, if so, creates a new, smaller, specified group.

20 One aspect of the invention provides a communications system
21 comprising an interrogator, and a plurality of wireless identification
22 devices configured to communicate with the interrogator in a
23 wireless fashion. The respective wireless identification devices
24 have a unique identification number. The interrogator is configured

1 to employ tree search and Aloha techniques to determine the unique
2 identification numbers of the different wireless identification devices
3 so as to be able to establish communications between the
4 interrogator and individual ones of the multiple wireless
5 identification devices without collision by multiple wireless
6 identification devices attempting to respond to the interrogator at
7 the same time.

8 Another aspect of the invention provides a system comprising
9 an interrogator configured to communicate to a selected one or
10 more of a number of communications devices, and a plurality of
11 communications devices. The devices are configured to select
12 random values. Respective devices choose random values
13 independently of random values selected by the other devices. The
14 interrogator is configured to transmit a command requesting devices
15 having random values within a specified group of random values to
16 respond, the specified group being less than or equal to the entire
17 set of random values. Devices receiving the command are
18 configured to respectively determine if their chosen random values
19 fall within the specified group and, if so, send a reply to the
20 interrogator within a randomly selected time slot of a number of
21 slots. If not, they do not send a reply. The interrogator is
22 configured to determine if a collision occurred between devices that
23 sent a reply and, if so, create a new, smaller, specified group.
24

1 One aspect of the invention provides a radio frequency
2 identification device comprising an integrated circuit including a
3 receiver, a transmitter, and a microprocessor. In one embodiment,
4 the integrated circuit is a monolithic single die single metal layer
5 integrated circuit including the receiver, the transmitter, and the
6 microprocessor. The device of this embodiment includes an active
7 transponder, instead of a transponder which relies on magnetic
8 coupling for power, and therefore has a much greater range.
9

10 BRIEF DESCRIPTION OF THE DRAWINGS

11 Preferred embodiments of the invention are described below
12 with reference to the following accompanying drawings.

13 Fig. 1 is a high level circuit schematic showing an
14 interrogator and a radio frequency identification device embodying
15 the invention.

16 Fig. 2 is a front view of a housing, in the form of a badge
17 or card, supporting the circuit of Fig. 1 according to one
18 embodiment the invention.

19 Fig. 3 is a front view of a housing supporting the circuit of
20 Fig. 1 according to another embodiment of the invention.

21 Fig. 4 is a diagram illustrating a tree splitting sort method
22 for establishing communication with a radio frequency identification
23 device in a field of a plurality of such devices, without collisions.
24

1 Fig. 5 is a time line plot illustrating operation of a slotted
2 Aloha scheme.

3 Fig 6. is a diagram illustrating using a combination of a tree
4 splitting sort method with an Aloha method for establishing
5 communication with a radio frequency identification device in a
6 field of a plurality of such devices.

7
8 **DETAILED DESCRIPTION OF THE PREFERRED**
9 **EMBODIMENTS**

10 This disclosure of the invention is submitted in furtherance
11 of the constitutional purposes of the U.S. Patent Laws "to promote
12 the progress of science and useful arts" (Article 1, Section 8).

13 Fig. 1 illustrates a wireless identification device 12 in
14 accordance with one embodiment of the invention. In the
15 illustrated embodiment, the wireless identification device is a radio
16 frequency data communication device 12, and includes RFID
17 circuitry 16. In the illustrated embodiment, the RFID circuitry is
18 defined by an integrated circuit as described in the above-
19 incorporated patent application 08/705,043, filed August 29, 1996.
20 Other embodiments are possible. A power source 18 is connected
21 to the integrated circuit 16 to supply power to the integrated
22 circuit 16. In one embodiment, the power source 18 comprises a
23 battery. The device 12 further includes at least one antenna 14
24

1 connected to the circuitry 16 for wireless or radio frequency
2 transmission and reception by the circuitry 16.

3 The device 12 transmits and receives radio frequency
4 communications to and from an interrogator 26. An exemplary
5 interrogator is described in U.S. Patent Application Serial No.
6 08/907,689, filed August 8, 1997 and incorporated herein by
7 reference. Preferably, the interrogator 26 includes an antenna 28,
8 as well as dedicated transmitting and receiving circuitry, similar to
9 that implemented on the integrated circuit 16.

10 Generally, the interrogator 26 transmits an interrogation signal
11 or command 27 via the antenna 28. The device 12 receives the
12 incoming interrogation signal via its antenna 14. Upon receiving
13 the signal 27, the device 12 responds by generating and
14 transmitting a responsive signal or reply 29. The responsive signal
15 29 typically includes information that uniquely identifies, or labels
16 the particular device 12 that is transmitting, so as to identify any
17 object or person with which the device 12 is associated.

18 Although only one device 12 is shown in Fig. 1, typically
19 there will be multiple devices 12 that correspond with the
20 interrogator 26, and the particular devices 12 that are in
21 communication with the interrogator 26 will typically change over
22 time. In the illustrated embodiment in Fig. 1, there is no
23 communication between multiple devices 12. Instead, the devices
24 12 respectively communicate with the interrogator 26. Multiple

1 devices 12 can be used in the same field of an interrogator 26
2 (i.e., within communications range of an interrogator 26).
3 Similarly, multiple interrogators 26 can be in proximity to one or
4 more of the devices 12.

5 The radio frequency data communication device 12 can be
6 included in any appropriate housing or packaging. Various methods
7 of manufacturing housings are described in commonly assigned U.S.
8 Patent Application Serial No. 08/800,037, filed February 13, 1997,
9 and incorporated herein by reference.

10 Fig. 2 shows but one embodiment in the form of a card or
11 badge 19 including the radio frequency data communication device
12 12, and a housing 11 including plastic or other suitable material.
13 In one embodiment, the front face of the badge has visual
14 identification features such as graphics, text, information found on
15 identification or credit cards, etc.

16 Fig. 3 illustrates but one alternative housing supporting the
17 device 12. More particularly, Fig. 3 shows a miniature housing
18 20 encasing the device 12 to define a tag which can be supported
19 by an object (e.g., hung from an object, affixed to an object,
20 etc.). Although two particular types of housings have been
21 disclosed, the device 12 can be included in any appropriate
22 housing.
23
24

1 If the power source 18 is a battery, the battery can take any
2 suitable form. Preferably, the battery type will be selected
3 depending on weight, size, and life requirements for a particular
4 application. In one embodiment, the battery 18 is a thin profile
5 or button-type cell forming a small, thin energy cell more
6 commonly utilized in watches and small electronic devices requiring
7 a thin profile. A conventional cell has a pair of electrodes, an
8 anode formed by one face and a cathode formed by an opposite
9 face. In an alternative embodiment, the power source 18 comprises
10 a series connected pair of cells. Instead of using a battery, any
11 suitable power source can be employed.

12 The circuitry 16 further includes a backscatter transmitter and
13 is configured to provide a responsive signal to the interrogator 26
14 by radio frequency. More particularly, the circuitry 16 includes
15 a transmitter, a receiver, and memory such as is described in U.S.
16 Patent Application Serial Number 08/705,043.

17 Radio frequency identification has emerged as a viable and
18 affordable alternative to tagging or labeling small to large
19 quantities of items. The interrogator 26 communicates with the
20 devices 12 via an RF link, so all transmissions by the interrogator
21 26 are heard simultaneously by all devices 12 within range.

22 If the interrogator 26 sends out a command requesting that all
23 devices 12 within range identify themselves, and gets a large
24 number of simultaneous replies, the interrogator 26 may not be able

1 to interpret any of these replies. Therefore, arbitration schemes
2 are provided.

3 If the interrogator 26 has prior knowledge of the
4 identification number of a device 12 which the interrogator 26 is
5 looking for, it can specify that a response is requested only from
6 the device 12 with that identification number. To target a
7 command at a specific device 12, (i.e., to initiate point-on-point
8 communication), the interrogator 26 must send a number identifying
9 a specific device 12 along with the command. At start-up, or in
10 a new or changing environment, these identification numbers are not
11 known by the interrogator 26. Therefore, the interrogator 26 must
12 identify all devices 12 in the field (within communication range)
13 such as by determining the identification numbers of the devices 12
14 in the field. After this is accomplished, point-to-point
15 communication can proceed as desired by the interrogator 26.

16 Generally speaking, RFID systems are a type of multiaccess
17 communication system. The distance between the interrogator 26
18 and devices 12 within the field is typically fairly short (e.g.,
19 several meters), so packet transmission time is determined primarily
20 by packet size and baud rate. Propagation delays are negligible.
21 In RFID systems, there is a potential for a large number of
22 transmitting devices 12 and there is a need for the interrogator 26
23 to work in a changing environment, where different devices 12 are
24 swapped in and out frequently (e.g., as inventory is added or

1 removed). The inventors have determined that, in such systems,
2 the use of random access methods work effectively for contention
3 resolution (i.e., for dealing with collisions between devices 12
4 attempting to respond to the interrogator 26 at the same time).

5 RFID systems have some characteristics that are different from
6 other communications systems. For example, one characteristic of
7 the illustrated RFID systems is that the devices 12 never
8 communicate without being prompted by the interrogator 26. This
9 is in contrast to typical multiaccess systems where the transmitting
10 units operate more independently. In addition, contention for the
11 communication medium is short lived as compared to the ongoing
12 nature of the problem in other multiaccess systems. For example,
13 in a RFID system, after the devices 12 have been identified, the
14 interrogator can communicate with them in a point-to-point fashion.
15 Thus, arbitration in a RFID system is a transient rather than
16 steady-state phenomenon. Further, the capability of a device 12 is
17 limited by practical restrictions on size, power, and cost. The
18 lifetime of a device 12 can often be measured in terms of number
19 of transmissions before battery power is lost. Therefore, one of
20 the most important measures of system performance in RFID
21 arbitration is total time required to arbitrate a set of devices 12.
22 Another measure is power consumed by the devices 12 during the
23 process. This is in contrast to the measures of throughput and
24 packet delay in other types of multiaccess systems.

Fig. 4 illustrates one arbitration scheme that can be employed for communication between the interrogator and devices 12. Although the arbitration system is being described in connection with a wireless identification system or RFID system, this and other arbitration schemes disclosed herein can be employed in any communication system. Generally, the interrogator 26 sends a command causing each device 12 of a potentially large number of responding devices 12 to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator 26 determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator 26 is able to conduct subsequent uninterrupted communication with devices 12, one at a time, by addressing only one device 12.

Three variables are used: an arbitration value (AVALUE), an arbitration mask (AMASK), and a random value ID (RV). The interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. The interrogator sends an arbitration value (AVALUE) and an arbitration mask (AMASK) to a set of devices 12. The receiving devices 12 evaluate the following equation:

1 (AMASK & AVALUE)==(AMASK & RV) wherein "&" is a bitwise
2 AND function, and wherein "==" is an equality function. If the
3 equation evaluates to "1" (TRUE), then the device 12 will reply.
4 If the equation evaluates to "0" (FALSE), then the device 12 will
5 not reply. By performing this in a structured manner, with the
6 number of bits in the arbitration mask being increased by one each
7 time, eventually a device 12 will respond with no collisions.
8 Thus, a binary search tree methodology is employed.

9 An example using actual numbers will now be provided using
10 only four bits, for simplicity, reference being made to Fig. 4. In
11 one embodiment, sixteen bits are used for AVALUE and AMASK,
12 respectively. Other numbers of bits can also be employed
13 depending, for example, on the number of devices 12 expected to
14 be encountered in a particular application, on desired cost points,
15 etc.

16 Assume, for this example, that there are two devices 12 in
17 the field, one with a random value (RV) of 1100 (binary), and
18 another with a random value (RV) of 1010 (binary). The
19 interrogator is trying to establish communications without collisions
20 being caused by the two devices 12 attempting to communicate at
21 the same time.

22 The interrogator sets AVALUE to 0000 (or all "don't care",
23 indicated by the character "X" in Fig. 4) and AMASK to 0000.
24 The interrogator transmits a command to all devices 12 requesting

1 that they identify themselves. Each of the devices 12 evaluate
2 $(AMASK \& AVALUE) == (AMASK \& RV)$ using the random value
3 RV that the respective devices 12 selected. If the equation
4 evaluates to "1" (TRUE), then the device 12 will reply. If the
5 equation evaluates to "0" (FALSE), then the device 12 will not
6 reply. In the first level of the illustrated tree, AMASK is 0000
7 and anything bitwise ANDed with all zeros results in all zeros, so
8 both the devices 12 in the field respond, and there is a collision.

9 Next, the interrogator sets AMASK to 0001 and AVALUE to
10 0000 and transmits an identify command. Both devices 12 in the
11 field have a zero for their least significant bit, and
12 $(AMASK \& AVALUE) == (AMASK \& RV)$ will be true for both
13 devices 12. For the device 12 with a random value of 1100, the
14 left side of the equation is evaluated as follows $(0001 \&$
15 $0000) = 0000$. The right side is evaluated as $(0001 \& 1100) = 0000$.
16 The left side equals the right side, so the equation is true for the
17 device 12 with the random value of 1100. For the device 12 with
18 a random value of 1010, the left side of the equation is evaluated
19 as $(0001 \& 0000) = 0000$. The right side is evaluated as $(0001 \&$
20 $1010) = 0000$. The left side equals the right side, so the equation
21 is true for the device 12 with the random value of 1010. Because
22 the equation is true for both devices 12 in the field, both devices
23 12 in the field respond, and there is another collision.

1 Recursively, the interrogator next sets AMASK to 0011 with
2 AVALUE still at 0000 and transmits an identify command.
3 $(AMASK \ \& \ AVALUE) == (AMASK \ \& \ RV)$ is evaluated for both
4 devices 12. For the device 12 with a random value of 1100, the
5 left side of the equation is evaluated as follows $(0011 \ \& \ 0000) = 0000$.
6 The right side is evaluated as $(0011 \ \& \ 1100) = 0000$.
7 The left side equals the right side, so the equation is true for the
8 device 12 with the random value of 1100, so this device 12
9 responds. For the device 12 with a random value of 1010, the
10 left side of the equation is evaluated as $(0011 \ \& \ 0000) = 0000$.
11 The right side is evaluated as $(0011 \ \& \ 1010) = 0010$. The left side
12 does not equal the right side, so the equation is false for the
13 device 12 with the random value of 1010, and this device 12 does
14 not respond. Therefore, there is no collision, and the interrogator
15 can determine the identity (e.g., an identification number) for the
16 device 12 that does respond.

17 De-recursion takes place, and the devices 12 to the right for
18 the same AMASK level are accessed by setting AVALUE at 0010
19 and using the same AMASK value 0011.

20 The device 12 with the random value of 1010 receives a
21 c o m m a n d a n d e v a l u a t e s t h e e q u a t i o n
22 $(AMASK \ \& \ AVALUE) == (AMASK \ \& \ RV)$. The left side of the
23 equation is evaluated as $(0011 \ \& \ 0010) = 0010$. The right side of
24 the equation is evaluated as $(0011 \ \& \ 1010) = 0010$. The right side

1 equals the left side, so the equation is true for the device 12 with
2 the random value of 1010. Because there are no other devices 12
3 in the subtree, a good reply is returned by the device 12 with the
4 random value of 1010. There is no collision, and the interrogator
5 can determine the identity (e.g., an identification number) for the
6 device 12 that does respond.

7 By recursion, what is meant is that a function makes a call
8 to itself. In other words, the function calls itself within the body
9 of the function. After the called function returns, de-recursion
10 takes place and execution continues at the place just after the
11 function call; i.e. at the beginning of the statement after the
12 function call.

13 For instance, consider a function that has four statements
14 (numbered 1,2,3,4) in it, and the second statement is a recursive
15 call. Assume that the fourth statement is a return statement. The
16 first time through the loop (iteration 1) the function executes the
17 statement 2 and (because it is a recursive call) calls itself causing
18 iteration 2 to occur. When iteration 2 gets to statement 2, it calls
19 itself making iteration 3. During execution in iteration 3 of
20 statement 1, assume that the function does a return. The
21 information that was saved on the stack from iteration 2 is loaded
22 and the function resumes execution at statement 3 (in iteration 2),
23 followed by the execution of statement 4 which is also a return
24 statement. Since there are no more statements in the function, the

1 function de-recursive to iteration 1. Iteration 1, had previously
2 recursively called itself in statement 2. Therefore, it now executes
3 statement 3 (in iteration 1). Following that it executes a return
4 at statement 4. Recursion is known in the art.

5 Consider the following code, which employs recursion, and
6 which can be used to implement operation of the method shown in
7 Fig. 4 and described above.

8
9 Arbitrate(AMASK, AVALUE)
10 {
11 collision=IdentifyCmnd(AMASK, AVALUE)
12 if (collision) then
13 {
14 /* recursive call for left side */
15 Arbitrate((AMASK<<1)+1, AVALUE)
16 /* recursive call for right side */
17 Arbitrate((AMASK<<1)+1, AVALUE+(AMASK+1))
18 } /* endif */
19 } /* return */
20

21 The symbol "<<" represents a bitwise left shift. "<<1"
22 means shift left by one place. Thus, 0001 << 1 would be 0010.
23 Note, however, that AMASK is originally called with a value of
24 zero, and 0000 << 1 is still 0000. Therefore, for the first
recursive call, AMASK = (AMASK << 1)+1. So for the first
recursive call, the value of AMASK is 0000+0001=0001. For the
second call, AMASK=(0001 << 1)+1=0010+1=0011. For the
third recursive call, AMASK=(0011 << 1)+1=0110+1=0111.

1 The routine generates values for AMASK and AVALUE to be
2 used by the interrogator in an identify command "IdentifyCmnd."
3 Note that the routine calls itself if there is a collision. De-
4 recursion occurs when there is no collision. AVALUE and AMASK
5 would have values such as the following assuming there are
6 collisions all the way down to the bottom of the tree.

AVALUE	AMASK
0000	0000
0000	0001
0000	0011
0000	0111
0000	1111*
1000	1111*
0100	0111
0100	1111*
1100	1111*

21 This sequence of AMASK, AVALUE binary numbers assumes
22 that there are collisions all the way down to the bottom of the
23 tree, at which point the Identify command sent by the interrogator
24

1 is finally successful so that no collision occurs. Rows in the table
2 for which the interrogator is successful in receiving a reply without
3 collision are marked with the symbol "*". Note that if the
4 Identify command was successful at, for example, the third line in
5 the table then the interrogator would stop going down that branch
6 of the tree and start down another, so the sequence would be as
7 shown in the following table.

AVALUE	AMASK
0000	0000
0000	0001
0000	0011*
0010	0011
...	...

18 This method is referred to as a splitting method. It works
19 by splitting groups of colliding devices 12 into subsets that are
20 resolved in turn. The splitting method can also be viewed as a
21 type of tree search. Each split moves the method one level deeper
22 in the tree. Either depth-first or breadth first traversals of the
23 tree can be employed.

Another arbitration method that can be employed is referred to as the "Aloha" method. In the Aloha method, every time a device 12 is involved in a collision, it waits a random period of time before retransmitting. This method can be improved by dividing time into equally sized slots and forcing transmissions to be aligned with one of these slots. This is referred to as "slotted Aloha." In operation, the interrogator asks all devices 12 in the field to transmit their identification numbers in the next time slot. If the response is garbled, the interrogator informs the devices 12 that a collision has occurred, and the slotted Aloha scheme is put into action. This means that each device 12 in the field responds within an arbitrary slot determined by a randomly selected value. In other words, in each successive time slot, the devices 12 decide to transmit their identification number with a certain probability.

The Aloha method is based on a system operated by the University of Hawaii. In 1971, the University of Hawaii began operation of a system named Aloha. A communication satellite was used to interconnect several university computers by use of a random access protocol. The system operates as follows. Users or devices transmit at any time they desire. After transmitting, a user listens for an acknowledgment from the receiver or interrogator. Transmissions from different users will sometimes overlap in time (collide), causing reception errors in the data in each of the contending messages. The errors are detected by the

1 receiver, and the receiver sends a negative acknowledgment to the
2 users. When a negative acknowledgment is received, the messages
3 are retransmitted by the colliding users after a random delay. If
4 the colliding users attempted to retransmit without the random
5 delay, they would collide again. If the user does not receive
6 either an acknowledgment or a negative acknowledgment within a
7 certain amount of time, the user "times out" and retransmits the
8 message.

9 In the slotted Aloha scheme, a sequence of coordination
10 pulses is broadcast to all stations (devices). As is the case with
11 the pure Aloha scheme, packet lengths are constant. Messages are
12 required to be sent in a slot time between synchronization pulses,
13 and can be started only at the beginning of a time slot. This
14 reduces the rate of collisions because only messages transmitted in
15 the same slot can interfere with one another. The retransmission
16 mode of the pure Aloha scheme is modified for slotted Aloha such
17 that if a negative acknowledgment occurs, the device retransmits
18 after a random delay of an integer number of slot times.

19 Fig. 5 illustrates operation of the slotted Aloha scheme. Fig.
20 5 shows a packet of data bits transmitted by a first device 12a,
21 which is substantially identical to the device 12. The interrogator
22 26 acknowledges receipt without collision, as indicated in Fig. 5
23 by the symbol ACK. Fig. 5 also shows devices 12b and 12c, also
24 substantially identical to the device 12, simultaneously transmitting

1 packets of data to the interrogator 26, resulting in a collision.
2 The interrogator returns a negative acknowledgment, as indicated in
3 Fig. 5 by the symbol NAK. The devices 12b and 12c then
4 respectively select random numbers, and retransmit after a time
5 delay corresponding to the selected random number. There is a
6 possibility that the devices 12b and 12c will again transmit at the
7 same times, causing another collision, but in that case they will
8 retransmit again using newly selected random numbers until there
9 is no collision.

10 Another form of Aloha scheme is called reservation-Aloha.
11 The reservation-Aloha system has two basic modes: an unreserved
12 mode, and a reserved mode.

13 In the unreserved mode, a time frame is established and
14 divided into a number of small reservation subslots. Users
15 (devices) use these subslots to reserve message slots. After
16 requesting a reservation, the user (device) listens for an
17 acknowledgment and a slot assignment.

18 In the reserved mode, a time frame is divided into a certain
19 number of slots whenever a reservation is made. All but the last
20 slot are used for message transmissions. The last slot is
21 subdivided into subslots to be used for reservations. Users
22 (devices) send message packets in their assigned portions of the
23 slots reserved for message transmissions.
24

Fig. 6 illustrates combining a tree sort method of a type such as the one shown in Fig. 4 with an Aloha method. Combining the two methods allows a minimal number of slots to be used and takes advantage of the conquer and divide approach of the tree sort method. The method shown in Fig. 6 proceeds in a manner similar to the manner described in connection with Fig. 4, except that devices 12 in the field that reply for the given AMASK and AVALUE, reply within a randomly selected time slot. This significantly reduces the number of collisions. In one embodiment, the reply includes the unique identification number of the particular device 12. In one embodiment, the reply includes the random value RV selected by the particular device 12. In one embodiment, the reply includes both the unique identification number of the particular device 12 as well as the random value RV selected by the same device 12.

In one embodiment, the same randomly selected time slot is used by a device 12 at different levels of the tree (i.e., for different values of AMASK and AVALUE). In another embodiment, different randomly selected times slots are used by a device 12 at different levels of the tree (i.e., for different values of AMASK and AVALUE). In one embodiment, a combination of these approaches is used. For example, one embodiment utilizes a method where the interrogator goes down the tree until some responses without collision are received, before the devices 12

1 re-randomize their Aloha random number. This can be classified
2 as an adaptive method. Other adaptive methods are possible. For
3 example, in one embodiment, the number of Aloha slots is reduced
4 at lower levels of the tree. The number of slots can be reduced
5 by the same number for each level down the tree, or by a number
6 that varies depending on the number of levels down the tree.
7 Thus, for example, the number of slots can remain constant through
8 a progression down the tree until some responses without collision
9 are received, at which point the number of slots is reduced.

10 Thus, this embodiment provides the advantages of both the
11 Aloha methods and the tree sorting methods of establishing
12 communications without collisions.

13 In another embodiment, levels of the search tree are skipped.
14 Skipping levels in the tree, after a collision caused by multiple
15 devices 12 responding, reduces the number of subsequent collisions
16 without adding significantly to the number of no replies. In real-
17 time systems, it is desirable to have quick arbitration sessions on
18 a set of devices 12 whose unique identification numbers are
19 unknown. Level skipping reduces the number of collisions, both
20 reducing arbitration time and conserving battery life on a set of
21 devices 12. In one embodiment, every other level is skipped. In
22 alternative embodiments, more than one level is skipped each time.

23 The trade off that must be considered in determining how
24 many (if any) levels to skip with each decent down the tree is as

1 follows. Skipping levels reduces the number of collisions, thus
2 saving battery power in the devices 12. Skipping deeper (skipping
3 more than one level) further reduces the number of collisions. The
4 more levels that are skipped, the greater the reduction in
5 collisions. However, skipping levels results in longer search times
6 because the number of queries (Identify commands) increases. The
7 more levels that are skipped, the longer the search times.
8 Skipping just one level has an almost negligible effect on search
9 time, but drastically reduces the number of collisions. If more
10 than one level is skipped, search time increases substantially.
11 Skipping every other level drastically reduces the number of
12 collisions and saves battery power without significantly increasing
13 the number of queries.

14 Level skipping methods are described in a commonly assigned
15 patent application (attorney docket MI40-117) naming Clifton W.
16 Wood, Jr. and Don Hush as inventors, titled "Method of
17 Addressing Messages, Method of Establishing Wireless
18 Communications, and Communications System," filed concurrently
19 herewith, and incorporated herein by reference.

20 In compliance with the statute, the invention has been
21 described in language more or less specific as to structural and
22 methodical features. It is to be understood, however, that the
23 invention is not limited to the specific features shown and
24 described, since the means herein disclosed comprise preferred

1 forms of putting the invention into effect. The invention is,
2 therefore, claimed in any of its forms or modifications within the
3 proper scope of the appended claims appropriately interpreted in
4 accordance with the doctrine of equivalents.
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24